HN

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/083,010	02/26/2002	Matthew Charles Priestley	MS190438.1	4314

27195 7590 01/20/2006

AMIN & TUROCY, LLP
24TH FLOOR, NATIONAL CITY CENTER
1900 EAST NINTH STREET
CLEVELAND, OH 44114

EXAMINER	
ABEDIN, SHANTO	
ART UNIT	PAPER NUMBER
2136	

DATE MAILED: 01/20/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 10/083,010	**Applicant(s)** PRIESTLEY ET AL.	
	Examiner Shanto M Z Abedin	**Art Unit** 2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE _03_ MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on _06 December 2005_.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) _1,3-18,20-29 and 31-33_ is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) _1,3-18,20-29 and 31-33_ is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on _26 February 2002_ is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _07/31/2002_.

4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application (PTO-152)

6) ☐ Other: _____.

DETAILED ACTION

Response to Amendment

1. Applicant's arguments/ amendments with respect to amended claims 1, 18, 27, 28, 31, 33, and their dependent claims filed on 12/06/2005 have been fully considered, but they are not persuasive. The examiner would like to point out that this action is made **FINAL** (MPEP 706.07a).

2. Examiner withdraws previous U.S.C. 101 rejections on claims 1-17, and 27-33.

3. Examiner further lists the prior arts made of record and not relied upon are considered closely pertinent to applicant's disclosure at the end of this office action (also see Form PTO-892).

4. Claims 1, 3-17, 18, 20-26, 27, 28, 29, 31, 32, and 33 were currently presented for the examination.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

5. Claim 20 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Regarding claim 20, it recites the limitation "The method of claim 19". Since claim 19 is currently cancelled or does not exist in the newly amended claim set, there is insufficient antecedent basis for this limitation in the claim. *Note, As best understood, examiner interprets as claim 20 is dependent on claim 18, and is treated accordingly.*

Response to Arguments

6. Applicant's arguments with respect to claims 1-33 have been considered but are moot in view of the new ground(s) of rejection.

7. a. Regarding claims 1 and 28, applicant argues that: Lee et al fails to disclose that the pass phrase is distributed separately from credentials. Claims 1 and 28 have been amended to incorporate the pass phrase being distributed separately from credentials.

b. Regarding claims 18, 27, and 33 applicant argues that: Lee et al fails to disclose that the executable and the pass phrase are transmitted to a system via different communication mediums. Claims 18 has been amended to incorporate the step of transmitting the executable and the pass phrase to a system via different communications mediums. Independent claims 27 and 33 recite similar limitations with respect to the transmission of the executable and the pass phrase to a system via different communication mediums.

c. Regarding claims 3-4, 17, 23, 29-30 applicant argues that: Lee et al fails to expressly or inherently disclose applicant's claimed invention as recited in independent claims 1, 18,27,28, and 33 (and claims 3-4, 17,23 and 29-30 which respectively depend there from).

d. Regarding claims 5-11, 18, 20 and 26, applicant argues that: The contention that separately distributing the pass phrase from the credentials would have been obvious in view of the teaching of Lee et al and Ramakrishnan constitutes nothing more than hindsight speculation. Moreover, the combination of Lee et al and Ramakrishnan does not teach the claimed invention.

e. Regarding claims 13-16, 21, 22,31, and 33, applicant argues that: Brainard does not make up for the aforementioned deficiencies of Lee et al with respect to independent claims 1, 18 and 31 (which claims 13-16, 21,22 and 32 depend there from).

f. Regarding claims 24 and 25, applicant argues that Chatani et al does not make up for the aforementioned deficiencies of Lee et al with respect to independent claim 18 (which claims 24 and 25 depend there from).

However, examiner disagrees with applicant.

Regarding argument (a), (b), and (c), applicant's arguments with respect to claims 1,3,4,17,18,23,27-30 and 33 have been considered but are moot in view of the new ground(s) of rejection (See office action below).

Regarding argument (d), examiner withdraws the previous rejections on claims 5-11, 18, 20 and 26 based upon prior art Lee et al and Ramakrisnan. However, applicant's arguments are moot in view of the new ground(s) of rejection (See office action below).

Regarding argument (e), applicant's arguments with respect to claims 13-16, 21, 22,31, and 33 have been considered but are moot in view of the new ground(s) of rejection (See office action below).

Regarding argument (f), applicant's arguments with respect to claims 24 and 25 have been considered but are moot in view of the new ground(s) of rejection (See office action below).

8. Based on the arguments set forth by the examiner for arguments (a)-(f), the independent claims 1, 18, 27, 28, 31 and 33 and their dependent claims stand rejected.

9. The examiner is not trying to teach the invention but is merely trying to interpret the claim language in its broadest and reasonable meanings. Therefore, the examiner asserts that the system of the prior arts Lee et al, Goldstone, and Brainard combined teach or suggest the subject matter as recited in independent claims 1, 18, 27, 28, 31 and 33.

Rejections

10. The text of those sections of the title 35, U. S. Code not included in this office action can be found in a prior Office action.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

11. Claims 1, 3-12, 17, 18, 20, 23, 27,28, 29 and 33 are rejected under USC 103 (a) as being unpatentable over Lee et al (" A secure electronic software distribution (ESD) protocol based on PKC", EC-Web 2000, LNCS 1875, pp. 63-71, 2000) in view of Goldstone (Pub No: US 2003/0142364 A1).

Regarding claim 1, Lee et al discloses a computer implemented system ((Section 2.2: Software based technologies; Section 3: Proposed ESD protocol; Figure 1: Overall architecture of proposed protocol) for processing credentials, comprising the following computer executable components:

a wrapper (Figure 1, element: Electronic License Packaging) that packages credentials associated with resources of a service (Section 2.2: Software based technologies; Section 3.1: Overall Architecture; Section 3.2: Secure Installation scheme; Figure 1: Overall architecture of proposed protocol; Figure 2: Secure installation procedure)[Lee et al discloses a merchant server comprising an electronic license packaging module that wraps the software to be downloaded in a package];

a pass phrase (a "secret" string shared only by authorization unit in client's computer and by the server, Figure 2, element: Elicense) employed in connection with generation of the wrapper, the pass phrase employed to facilitate access to the credentials, the credentials employed to facilitate access to the resources to the server (Section 2.2: Software based technologies; Section 3.1: Overall Architecture; Section 3.2: Secure Installation scheme; Figure 1: Overall architecture of proposed protocol; Figure 2: Secure installation procedure) [Lee et al discloses a locked wrapper to package software that can be unlocked using an Electronic License Certificate (ELC) comprising a "secret" component (a random string shared by only the server and authentication module in client's computer). A person with the ordinary skill in the art will be able to interpret Lee et al's "secret" component as a pass phrase].

Lee et al does not disclose expressly the pass phrase distributed separately from the credentials. However, Goldstone discloses the pass phrase distributed separately from the credentials (Page 3, Par. [0029], [0034]; Page 8, Par. [0098]; Page 9, claims 5-7; Goldstone teaches a password/ shared secret and an electronic message are distributed separately in a message retrieval system; examiner interprets that such "password/ shared secret" can also be implemented as a pass-phrase; examiner further interprets "electronic message" as credential).

Goldstone and Lee et al are analogous art because they are from the same field of endeavor of secure electronic data/ software transmission and retrieval. At the time of invention it would have been obvious to a person of ordinary skill in the art to combine the teaching of Goldstone with Lee et al for distributing the pass phrase separately from the credential. Motivation for doing so would have been that such separate distribution of password/ pass-phrase and credential/ message/ is commonly used in the field of endeavor as a safeguard against eavesdropping, or that such mechanism provide extra security in secure message/ data transmission (Goldstone, Par. [0098]).

Regarding claim 18, it recites the limitations of claim 1, therefore, it is rejected applying as above rejecting claim1, furthermore, Lee et al discloses a method to facilitate a security connection between entities (Section 3: Proposed ESD Protocol), comprising:

Generating a strong password (Section 3.1: Overall Architecture; Section 3.2: Secure Installation Scheme; Figure 2, element: E-license, passwd) [Lee et al discloses generation of an electronic license certificate comprising password];

Generating a pass phrase (Section 3.1: Overall Architecture; Section 3.2: Secure Installation Scheme; Figure 2, element: E-license, secret) [Lee et al discloses generation of an electronic license certificate comprising a "secret" string. The "secret" is shared only between the authentication module and the server and is a random string. A person with ordinary skill in the art would be able to interpret the "secret" as a pass phrase];

Wrapping the password cryptographically via the pass phrase (Section 3.1: Overall Architecture; Section 3.2: Secure Installation Scheme; Figure 2, element: E-license, H(secret, customer_ID, passwd)) [Lee et al discloses generation of an electronic license certificate also comprising cryptographic function H (secret, customer_id, passwd) that cryptographically wraps the secret string] ;

Storing the wrapped password in an executable (Section 3.1: Overall Architecture; Section 3.2: Secure Installation Scheme; Figure 1, element: merchant server, JDBC data source, electronic license processing) [Lee et al discloses use of JDBC component, a storing facility and "electronic license packaging" module (which contains password in it) to wrap the packaged software].

Lee et al does not disclose expressly transmitting the executable and the pass-phrase to a system via different communications mediums. However, Goldstone discloses transmitting the executable and the pass-phrase to a system via different communications mediums (Page 3, Par. [0029], [0034]; Page 8, Par. [0098]; Page 9, claims 5-7; Goldstone teaches a password/ shared secret and an electronic message are distributed separately in a message retrieval system; examiner interprets that such "password/ shared secret" can also be implemented as a pass-phrase; examiner further interprets "electronic message" as executable).

Goldstone and Lee et al are analogous art because they are from the same field of endeavor of secure electronic data/ software transmission and retrieval. At the time of invention it would have been obvious to a person of ordinary skill in the art to combine the teaching of Goldstone with Lee et al for distributing the pass phrase separately from the executable. Motivation for doing so would have been that such separate distribution of password/ pass-phrase and data/ executable is commonly used in the field of endeavor as a safeguard against eavesdropping, or that such mechanism provide extra security in secure message/ data transmission (Goldstone, Par. [0098]).

Regarding claim 27, it recites the limitations of claims 1, and 18, therefore, it is rejected applying as above rejecting claims 1 and 18, furthermore, Lee et al discloses a computer executable system to facilitate a security relationship between parties (Section 3: Proposed ESD Protocol), comprising:

Computer implemented means for generating a strong password (Section 3.1: Overall Architecture; Section 3.2: Secure Installation Scheme; Figure 2, element: E-license, passwd) [Lee et al teaches generation of an electronic license certificate comprising password in it];

Computer implemented means for generating a pass phrase (Section 3.1: Overall Architecture; Section 3.2: Secure Installation Scheme; Figure 2, element: E-license, secret) [Lee et al discloses generation of an electronic license certificate comprising a secret string that works as as a pass phrase];

Computer implemented means for generating a package (Section 2.2: Software based technologies; Section 3.1: Overall Architecture; Figure 1, element: Electronic License Packaging) [Lee et al discloses a electronic license packaging module to package software in a wrapper]

Computer implemented means for storing the password in the package (Section 3.1: Overall Architecture; Section 3.2: Secure Installation Scheme; Figure 2, element: E-license, H(secret, customer_ID, passwd); Figure 1, element: merchant server, JDBC data source, electronic license processing) [Lee et al discloses an electronic license certificate (used to package the software) comprising a cryptographic function H (secret, customer_id, passwd) that securely store the password.]

Computer implemented means for locking the package with the pass –phrase (Section 2.2: Software based technologies; Section 3.1: Overall Architecture; Section 3.2: Secure Installation Scheme; Figure 1, element: merchant server, JDBC data source, electronic license processing) [Lee et al discloses a H function (as a part of electronic license certificate) comprising a password, and a pass phrase like "secret" string that is used to lock the wrapper containing packaged software].

Lee et al does not disclose expressly transmitting the package and the passphrase to a system via different communication mediums. However, Goldstone discloses transmitting the package and the passphrase to a system via different communication mediums (Page 3, Par. [0029]; Page 8, Par. [0098]; Page 9, claims 5-7).

Regarding claim 28, it recites the limitations of claim 27, therefore, it is rejected applying as above rejecting claim 27, furthermore, Lee et al discloses a computer readable medium having stored thereon a signal to communicate security data between at least two nodes (Section 3.1: Overall architecture; Section 3.2: Secure Installation scheme; Figure 1, element: electronic license packaging; figure 2: E license) comprising: a first data packet comprising:

A password component employed to establish a trust relationship between at least two nodes (Section 3.1: Overall Architecture; Section 3.2: Secure Installation Scheme; Figure 2, element: E-license, Figure 2, element: E-license, H(secret, customer_ID, passwd) [Lee et al discloses an electronic license certificate which contains a cryptographic function H (secret, customer_ID, passwd) comprising password in it];

A wrapper field employed to encapsulate the password, the wrapper field mediating access to the password (Section 2.2: Software based technologies; Section 3.1: Overall Architecture; Section 3.2: Secure Installation scheme; Figure 1, element: Electronic license packaging; Figure 2, element: e-license) [Lee et al discloses generation of an electronic license certificate which contains a cryptographic function H (secret, customer_id, passwd) which cryptographically secure the password. A person of the ordinary skill in the art would be able to design a wrapper field to encapsulate the password by using similar technique used by Lee et al to form H (secret, customer_id, passwd)];

A second data packet comprising:

A pass phrase employed to unlock the wrapper field (Page 65, lines 1-5; Page 67, lines 5-12; Fig 2, element: E license; Lee et al teaches employing an e-license comprising a "secret" to unlock the software package).

Lee et al does not disclose expressly the pass phrase distributed separately from the wrapper field. However, Goldstone discloses the pass phrase distributed separately from the wrapper field (Page 3, Par. [0029]; Page 8, Par. [0098]; Page 9, claims 5-7).

Regarding claim 33, it recites the limitations of claim 28, therefore, it is rejected applying as above rejecting claim 28, furthermore, Lee et al discloses a computer readable medium having stored thereon a data structure (Section 3.1: Overall Architecture; Section 3.2: Secure Installation Scheme; Fig 2, element: e- license; Fig 3, element: executable packaged file, decryption of encrypted exe file and software execution thread), comprising:

A first data field containing cryptographic data associated with a password (Page 67, lines 1-18; Fig 2, element: E-license) [Lee et al teaches AA storing password data used to create a cryptographic hash digest];

A second data field (secret field of H function) containing cryptographic data associated with a pass phrase, the pass phrase employed to migrate exposure of the password to non trusted entitie (Page 67, lines 1-18; Fig 2, element: E-license) [Lee et al teaches AA storing "secret" data used to create a cryptographic hash digest];

A third data field containing a wrapper employed to encapsulate the password (Page 67, lines 1-18; Fig 2, element: E-license) [Lee et al teaches AA generating a cryptographic hash digest, H to encapsulate pass phrase and password];

Lee et al does not disclose expressly the wrapper distributed separately from the passphrase to facilitate a security connection between entities. However, Goldstone discloses the wrapper distributed separately from the pass phrase to facilitate a security connection between entities (Page 8, Par. [0098]; Page 9, claims 5-7).

Regarding claim 3, it is rejected applying as above rejecting claim 1, furthermore, Lee et al discloses the credentials providing stronger encryption than the pass phrase (Section 3.1: Overall architecture; Section 3.2: Secure Installation scheme) [Lee et al discloses that second component of the electronic license certificate (that implies to credentials) are encrypted by using a public key and server's private key. A person with the ordinary skill in the art can conclude that this type of public and private key encryption is usually stronger (128 bit or more) than the random string (recited in Lee et al) or the key crunching algorithm (usually 64 bit encryption) to generate random string from the pass phrase or a secret string (cross reference, "Applied cryptography" by Bruce Schneier, second edition, Wiley, 1996).]

Regarding claim 4, it is rejected applying as above rejecting claim 3, furthermore, Lee et al teaches that credentials are encrypted with greater than 100 bits of encryption (Section 1: Introduction, Paragraph 3; Section 3.1: Overall Architecture, Paragraph 2; Section 3.2: Secure Installation scheme, Paragraph 1)[Lee et al teaches use of encryption schemes such as Diffie Hellman, RSA, MD5, and SHA – all of them usually use greater than 100 bits of encryption (recited in cross reference, "Applied cryptography" by Bruce Schneier, second edition, Wiley, 1996)].

Regarding claim 5 and 9, Lee et al discloses a system of claim 3 (Section 3.1: Overall architecture; Section 3.2: Secure Installation scheme).

Lee et al does not disclose expressly that the pass – phrase having human readable, and alpha – numeric characteristics. However, Goldstone discloses the pass – phrase having human readable, and alpha – numeric characteristics (Page 3, Par. [0029]; Page 7, Par. [0075], [0076]; alpha numeric and voice recognizable password/ shared secret key);

Goldstone and and Lee et al are analogous art because they are from the same field of endeavor of secure electronic data/ software transmission and retrieval. At the time of invention it would have been obvious to a person of ordinary skill in the art to combine the teaching of Goldstone with Lee et al to design a pass phrase that is human readable, alpha – numeric and can be displayed on the screen. The motivation for doing so would simply been that such human readable and alpha numeric pass phrase is convenient for client's use and could be generated from either client or server side conveniently and efficiently.

Regarding claim 6, 7, and 8, Lee et al discloses a system of claim 1 (Section 2.2: Software based technologies; Section 3: Proposed ESD protocol; Figure 1: Overall architecture of proposed protocol).

Lee et al does not disclose expressly that one or more partners request access to the resources, or partners store and distribute the credentials. However, Goldstone discloses one or more partners request access to the resources, or partners store and distribute the credentials (Fig 2, element 10: sender, element 30: recipient's email server, element 40: mobile recipient; Page 2, Par. [0010], [0011]; Page 4, Par. [0038]).

Goldstone and Lee et al are analogous art because they are from the same field of endeavor of secure electronic data/ software transmission and retrieval. At the time of invention it would have been obvious to a person of ordinary skill in the art to combine the teaching of Goldstone with Lee et al for utilizing a pass phrase base wrapper for credential security in a system involving multiple partners facilitating users' need. The motivation for doing so would been that content and original server confidentiality are highly desirable in Internet (WAN) based system.

Regarding claim 10, 11, Lee et al discloses a system of claim 1 (Section 2.2: Software based technologies; Section 3: Proposed ESD protocol; Figure 1: Overall architecture of proposed protocol).

Lee et al does not disclose expressly use of that pass phrase over a SSL connection or in a VPN environment. However, Goldstone discloses use of that pass phrase over a SSL connection or in a VPN environment (Page 6, Par. [0058]; Page 8, Par. [0091]).

Goldstone and Lee et al are analogous art because they are from the same field of endeavor of secure electronic data/ software transmission and retrieval. At the time of invention it would have been obvious to a person of ordinary skill in the art to combine the teaching of Goldstone with Lee et al for utilizing a pass phrase base wrapper for credential security in a system involving SSL connection or VPN. The motivation for doing so would been that a SSL connection/ secure communication channel, or VPN provides further content security while transmitted through a network.

Regarding claim 12 is rejected applied as above rejecting claim 11, furthermore Lee et al discloses issuing an Electronic License Certificate (Section 3.1: Overall Architecture; Section 3.2: Secure Installation Scheme; Figure 1, element: certificate) by merchant server, and obtaining a public key certificate from a third party Certificate Authority (Section 3.1: Overall architecture, Figure 1, element CA) to facilitate secure communication between merchant server and customer.

Regarding claim 17, it is rejected applying as above rejecting claim 1, furthermore, Lee et al discloses a computer readable medium having computer executable instructions stored thereon to perform at least one of processing and generation of the wrapper and the pass phrase (Section 2.2: Software based technologies; Section 3.1: Overall architecture; Figure 1, element: electronic license packaging) [Lee et al teaches use of JDBC component "electronic license packaging" to package and email the wrapped electronic license (which contains a "secret" string as pass phrase) to customer].

Regarding claim 20, it recites the limitation of claim 18, therefore, it is rejected applying as above rejecting claim 18, furthermore, although Lee et al discloses a pass phrase based encryption/ decryption mechanism to lock/ unlock a password (Page 65, lines 1-10; Page 67, Lines 1-15; Fig 2, element : E license; Fig 3, decryption of encrypted exe file; AA to unlock/ decrypt exe file using E license; E license comprising a hash digest containing "secret" and password; AA having "secret"; examiner interprets either a "secret" or a "private key" can be used to decrypt such encrypted executables or a wrapped password).

Regarding claim 23, it is rejected applying as above rejecting claim 18, furthermore, Lee et al discloses a method of limiting access to the executables (Section 2.2: Software based technologies; Section 3.3: Illegal copy protection mechanism; Figure 3: Illegal copy protection protocol using multi thread). [Lee et al teaches use of an authentication server to limit access to the executable packages]

Regarding claim 29, it is rejected applying as above rejecting claim 28, furthermore, Lee et al discloses a wrapper field being cryptographically weaker than the password (Section 3.1: Overall architecture; Section 3.2: Secure Installation scheme) [Lee et al discloses that password and other credentials in electronic license certificate are encrypted by using a public key and server's private key. A person with the ordinary skill in the art can conclude that this type of public and private key encryption is usually stronger (128 bit or more) than the random string (recited in Lee et al) or the key crunching algorithm (usually 64 bit encryption) to generate random string from the pass phrase or a secret string (used for wrapper field) (cross reference, "Applied cryptography" by Bruce Schneier, second edition, Wiley, 1996)].

12. Claims 13 – 16, 21, 22, 31, and 32 are rejected under 35 USC 103 (a) as being unpatentable over Lee et al (" A secure electronic software distribution (ESD) protocol based on PKC", EC-Web 2000, LNCS 1875, pp. 63-71, 2000) in view of Goldstone (Pub No: US 2003/0142364 A1) further in view of Brainard (" SecurSight: An overview for secure information access", RSA Laboratories).

Regarding claim 31, Lee et al discloses a computer implemented system to establish a trust relationship, comprising the following computer executable components:

A wrapper generated by the service to package the credentials (Section 2.2: Software based technologies; Section 3.2: Overall Architecture; Figure 1, element: Electronic License Packaging, producer, merchant server)[Lee et al discloses a wrapper generated by merchant server (associated with a producer module) to package software];

A pass phrase employed to generate the wrapper and mediate access to the service (Section 2.2: Software based technologies; Section 3.2: Overall Architecture; Figure 1: Overall Architecture of proposed protocol) [Lee et al teaches a secret string within an electronic license certificate which is used to lock the wrapper containing packaged software, and such certificate is used to mediate access to the resources];

Lee et al does not disclose expressly a service that controls one or more resources, the service issues credentials to facilitate access to the resources, and the pass phrase distributed separately from credentials. However, Brainard teaches a security services comprising a manager module that issues Privilege Attribute Certificates to facilitate desktop's access to the resources.

Furthermore, Goldstone discloses the pass phrase distributed separately from credentials (Page 3, Par. [0029]; Page 8, Par. [0098]; Page 9, claims 5-7).

Goldstone, Brainard, and Lee et al are analogous art because they are from the same field of endeavor of transmission and access of secure information. At the time of invention it would have been obvious to a person of ordinary skill in the art to combine the teaching of Goldstone with the modified Lee et al -Brainard system for designing a service which issues credentials to mediate users' access to the resources and distribute pass phrase separately from credential. The motivation for doing so would been that such separate transmission of pass-phrase and credential provides extra security in secure message/ data transmission (Goldstone, Par. [0098]), and that such issuing of credentials for accessing resources is needed for authentication purpose(Brainard, Page 1, Section 1.1, Col 2, lines 30-37).

Regarding claim 13 and 14, Lee et al discloses a system of claim 1(Section 2.2: Software based technologies; Section 3: Proposed ESD protocol; Figure 1: Overall architecture of proposed protocol).

Lee et al does not disclose expressly a platform provisioning service, or such service being associated with a partner including a service provider and tenant. However, Brainard teaches a system of SecurSight authentication service which includes a manager, application server, client desktop, and directory services for external resources (Section 1.1: SecurSight Design Principal; Section 1.2: Component; Section 3: Authorization; Figure 5: PAC Usage). A person with ordinary skill in the art can design a platform provisioning service by using similar technique used in Brainard's manager component (that will act as both the authentication service and as the long term repository for users' access rights) of the SecurSight authentication service. A person with ordinary skill in the art can also implement a system comprising provisional services, client, and service provider by using similar technique used in Brainard's system consist of manager, desktop, and application server (Figure 5: PAC usage). Brainard's enterprise network resources and applications imply capability of performing billing, financial, or accounting functions.

Goldstone, Brainard, and Lee et al are analogous art because they are from the same field of endeavor of transmission and access of secure information. At the time of invention it would have been obvious to a person of ordinary skill in the art to combine the teaching of Brainard with Lee et al – Goldstone system for designing system of claim 1 further comprising platform provision service, partners, and service providers in order to facilitate network or enterprise application/ resources to the users efficiently and securely.

Regarding claim 15 is rejected applied as above rejecting claim 14, furthermore Lee et al discloses a "secret" string as a part of Electronic License Certificate (Section 3.1: Overall Architecture; Section 3.2: Secure Installation Scheme; Figure 1, element: certificate) that is used to unlock credentials and achieve access to the services (Section 2.2: Software based technologies, Paragraph 1;Section 3.2: Secure Installation scheme, Paragraph 2) .

Regarding claim 16 is rejected applied as above rejecting claim 14, furthermore Lee et al discloses a system associated with ecommerce technology (Section 1: Introduction, Paragraph 1 and 2) and use web browser to present the credentials to the client (Section 4: Comparison with existing models, Table 1) that is used to unlock credentials and achieve access to the services (Section 2.2: Software based technologies, Paragraph 1;Section 3.2: Secure Installation scheme, Paragraph 2).

Regarding claim 21, Lee et al discloses a system of claim 18.

Lee et al does not expressly teaches requesting a secure socket layer (SSL) connection or presenting an SSL certificate in response to the request. However, Brainard teaches requesting a secure socket layer(SSL) connection (Section 3.3: Use of PACs by connect agent; Section 4.2: Certificate Validation Service) and presenting an SSL certificate in response to the request(Section 3.3: Use of PACs by connect agent; Section 4.2: Certificate Validation Service)[Brainard teaches a desktop requesting for SSL connection with application server, and presenting a certificate to certificate validation service for validation.]

Goldstone, Brainard, and Lee et al are analogous art because they are from the same field of endeavor of transmission and access of secure information. At the time of invention it would have been obvious to a person of ordinary skill in the art to combine the teaching of Brainard with the modified Lee et al – Goldstone system for using a SSL connection and using a SSL certificate for authentication purpose. The motivation for doing so would been that SSL connection and use of SSL certificates are commonly practiced in secure network communication.

Regarding claim 22 is rejected applied as above rejecting claim 21, furthermore Brainard teaches a method comprising at least one of:

Verifying an SSL certificate (Section 3.3: Use of PACs by connect agent; Section 4.2: Certificate Validation Service)[Brainard teaches an application access agent and a certificate validation service to validate SSL certificates];

Requesting a Universal Resource Locator (URL) from a listener(Section 2.4: Comparison with other authenticators)[Brainard teaches obtaining web browser based credentials which essentially refers to use of an URL] ;

Presenting authentication credentials to a receiver (Section 3.3: Use of PACs by connect agent; Section 4.2: Certificate Validation Service)[Brainard teaches desktop presenting a certificate to be validated by the certificate validation service.];

Logging in a caller to an account (Section 3.1: PAC definition; Section 3.3: use of PACs by connect agents) [Brainard teaches a connect agent that initiates a client's access to an account after certificates are validated.]

Regarding claim 32, it is rejected applying as above rejecting claim 31, furthermore, Brainard discloses a manager module that perform as provisioning service, and issues credentials to authenticate users to access resources (Section 1.1: SecurSight Design Principal; Section 1.2: Component; Section 3: Authorization; Figure 5: PAC Usage).

13. Claim 24 and 25 are rejected under 35 USC 103 (a) as being unpatentable over Lee et al (" A secure electronic software distribution (ESD) protocol based on PKC" EC-Web 2000, LNCS 1875, pp. 63-71, 2000) in view of Goldstone (Pub No: US 2003/0142364 A1), further in view of Chatani et al (Pub No: US 2002/0104019 A1)

Regarding claim 24, it recites the limitation of claim 18, therefore, it is rejected applying as above rejecting claim 18, furthermore, Lee et al does not expressly discloses a method of setting up account privileges or designing account contacts or verifying the contacts. However, Chatani discloses method comprising at least one of:

Setting up account privileges (Fig 2B: element 224: User Info, element 240: Purchase info; Fig 1, element 102; Page 3, Paragraph [0027]; Page 6, Paragraph [0048] and [0049]) [Chatani teaches a user account to store necessary users' and purchase information in server that are used to authorize the resources. Person with ordinary skill in the art can use a similar technique as Chatani's to set up an account privileges method];

Designating account contacts (Fig 2B: element 224: User Info; Page 6, Paragraph [0048] and [0049]) Chatani teaches storing necessary user information in server. Person with ordinary skill in the art can store account contact using Chatani's teachings];

Verifying the contacts (Fig 2B: element 224: User Info; Page 6, Paragraph [0045], [0048] and [0049]) [Chatani teaches a server to verify user's purchage information. A person with ordinary skill in art can use a similar technique as Chatani's to verify the contacts].

Chatani, Goldstone and Lee et al are analogous art because they are from the same field of endeavor of secure software/ data transmission or distribution. At the time of invention it would have been obvious to a person of ordinary skill in the art to combine the teaching of Chatani with the modified Lee et al – Goldstone system for setting up an account privileges and verifying the contact associated with that account. The motivation for doing so would been simply that such user authentication is commonly practiced in the field of endeavor.

Regarding claim 25 is rejected applied as above rejecting claim 24. Furthermore, Lee et al does not expressly discloses a method of verbally communicating the password. However, Chatani discloses a method comprising verbally communicating the password (Figure 3A, element 314; Page 3, Paragraph [0025]; Page 5, Paragraph [0037], Paragraph [0038], Paragraph [0041]) [Chatani teaches using a telephone for inputing alphanumeric ID and for transmitting voice commands]

Chatani, Goldstone and Lee et al are analogous art because they are from the same field of endeavor of secure software/ data transmission or distribution. A person with ordinary skill in the art would modify the system of Chatani with the modified Lee et al- Goldstone system to verbally communicate the pass phrase in order to provide an alternative means for communicating the password and to maintain reliability of the system.

Conclusion

14. The following prior arts made of record and not relied upon are considered pertinent to applicant's disclosure. See Form PTO-892.

Prior art US 2002/0059144 A1 discloses a secure content delivery in a billing/ accounting system involving locking/ unlocking a secure package using a pass-phrase. System further utilizes encrypting/ decrypting a private key or a password using a pass-phrase, and encrypting/ decrypting secure data with the private key. System further utilizes SSL connection, certificates, and hashed certificate and digest.

Prior art US 5825300 discloses a method of protected distribution of keying and certificate materials utilizing separate communication channels.

Prior art US 2001/0011254 A1 discloses a method of protecting software/ executables from unlicensed use utilizing user key generated by random numbers, wherein software, key and license information is distributed in plurality of secure channels.

Prior art US 6343361 B1 discloses a system for electronic communication comprising generating a displayable pass phrase string which is used to access encoded information, and wherein a password entry field is associated with the pass phrase.

"Applied Cryptography", Bruce Schneier, pp 174, Second edition, Wiley, 1996 discloses cryptographic strength and nature of a passphrase.

"Tactical Network Security", Stuart Jacobs, IEEE, 1999 discloses a "secret" key algorithm wherein a "secret" key is used to create a secure message digest.

15. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Shanto M Z Abedin whose telephone number is 571-272-3551. The examiner can normally be reached on M-F from 9:00 AM to 5:30 PM. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh, can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Shanto M. Z. Abedin
Art Unit: 2136

Primary Examiner
AU 2131
1/16/06